CYBERCRIME AND INSURANCE: THE KEY ISSUES

Alan Rutkin, Robert Tugander, and Gregory J. Klubok Rivkin Radler LLP

Cyberattacks are becoming more common each year. Hardly a month goes by without the hacking of a major company. First American Title Insurance Company is the latest victim of a major data breach. This past May, it revealed that more than 885 million customer records were exposed due to a security flaw.

Cybercrime occurs in many forms. And criminals keep coming up with new and more sophisticated schemes to steal personal identities and funds.

When a new risk emerges, new insurance coverage issues follow. Several complicating factors make this new area of insurance law look a little bit like the Wild West: (1) cybercrimes require courts to fit new technologies into old categories, (2) cyber claims involve new and different policy forms, and (3) computer fraud policies often involve factually intensive questions. Most cases revolve around one or more of the following issues: authorization, causation, act, or injury.

AUTHORIZATION

Typically, insurance coverage for cyberattacks is limited to losses caused by someone who was not authorized to use the policyholder's computer system, i.e., hackers. In other words, the bad actor must have broken into the computer system. That is a higher threshold than *using* a computer; the bad actor must have *broken into* the computer system. That may seem like a fine distinction, but it really isn't. Practically everyone knows how to *use* a computer, but few know how to *hack into* one. The perpetrator, therefore, must not be authorized to access the computer system.

What about when an authorized person, such as an employee or agent, uses a policyholder's computer system to perform an unauthorized act? The policyholder is out of luck. Coverage is usually limited to losses caused by unauthorized users, and courts typically enforce this restriction, even where the authorized person was deceived.[1] Unauthorized acts by authorized persons are simply not covered by most cyber policies.

CAUSATION

Causation is a tough concept in the cyber insurance field. Often, cybercrime involves a series of steps to complete the fraudulent scheme. One or more of these steps may entail the use of a computer, but not all. In the cyber insurance field, most policies have a qualifier: They only cover "direct loss" from the use of a computer.

When is a loss direct? Different courts

have come to different conclusions, and there is no consensus. Some courts have held that the actual use of the computer must be, in effect, the final act to cause the loss.

Other courts have equated direct loss with a proximate cause requirement, which is much more policyholder-friendly. A proximate cause means a substantial cause; it does not have to be the last act in the cyber scheme. And there can be more than one proximate cause. A proximate cause analysis is malleable, giving courts flexibility in reaching a desired outcome.

An example is *Medidata Solutions*, which involved a fraudulent impersonation scheme.[2] Employees were tricked into wiring money to a phony account by spoofed emails and phone calls. The court held that there was a direct loss, as the spoofed emails set in motion a chain of events that culminated in the fraudulent transfer.

ACT

Most coverage litigation in the cyber context has concerned whether there was an act within the policy terms. Spoofing, hacking, and publishing are some examples.

Liability policies typically require that the injury-causing event be unintentional. They cover accidents, which, by their nature, are not intentional. Punching or shooting someone are classic examples of intentional conduct that is not covered, as injury necessarily flows from the act.

In the cyber context, the policyholder is often the victim of a devious scheme designed to steal money or information. But the policyholder is sometimes liable for its own intentional cyber acts. A real-life example happened when a dentist sought coverage after she posted fake online reviews of another dentist and was sued for defamation.[3] In another case, a policyholder, among other things, hacked an acquaintance's computer.[4] In both instances, there was no coverage because the acts were, rather plainly, committed intentionally.

Some policies also provide coverage when a publication causes injury. Typically, a publication injury is one that defames someone, steals someone else's ideas, or otherwise causes financial harm. There is a low threshold for publication in the cyber context: If it is available for online viewing, it has been published.[5] But the policyholder must be the one who did the publishing. In one case, a hacker stole information from the policyholder and published it. The policyholder sought coverage as a publication injury. The court recognized that a wide-scale data breach was a publication. But there was no coverage because the policyholder did not publish the information; the hacker did.[6]

INJURY

Policyholders have sometimes looked to their commercial general liability policies for coverage for cyber liabilities. Specifically, policyholders look to the personal and advertising injury, and property damage coverages.

Property damage coverage typically applies to tangible property. In the cyber context, that raises an interesting question: Is data tangible? An early case drew a distinction between software, which is intangible, and the tangible hardware used to operate it (like the physical computer).[7] Hardware, the court explained, merely reads the instructions given to it by software. Even if the intangible software is corrupted, the court reasoned, the tangible hardware can still perform as it is supposed to by reading the software's instructions; the software is just sending bad instructions. "By analogy," the court explained, "when the combination to a combination lock is forgotten or changed, the lock becomes useless, but the lock is not physically damaged."[8]

But courts are split on this; in fact, one court held that software "has physical existence . . . and can be perceived by the senses."[9] Quite frankly, that reasoning doesn't seem to make much sense.

Personal and advertising injury coverage applies to certain offenses, including injury caused through the publication of material that violates a person's right to privacy. In one case, computer tapes containing sensitive employee information fell out of a van and landed on a highway during transport. The tapes were not recovered. The court found this provision inapplicable because there was no evidence that anyone ever accessed the confidential information on the tapes.[10]

Turning to cyber policies, they typically require that the party making the claim against the insured be the one who actually suffered the privacy injury. In one case, hackers stole credit card information from a popular restaurant chain. An intermediary, who processed customers' credit card payments for the restaurant, requested that the restaurant pay the penalties imposed by the card issuer following the breach. The restaurant sought coverage under its cybersecurity policy, which covered claims for privacy injuries. Under the definition of "privacy injury," the person whose private personal information was accessed must have also sustained the complained-of injury. The claim was not covered because the service provider itself did not suffer a privacy injury. [11]

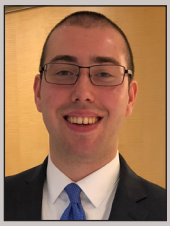
CONCLUSION

Cyber issues in the insurance context will continue to evolve, as the issues are fairly new. Complicating this body of law is the fact that different insurers use different policy language, and policyholders have sought coverage under various types of policies. A few trends, though, have emerged. Courts generally enforce clear restrictions on coverage when it comes to authorization and intentional misconduct. But policyholders typically win on publication issues.

As technology advances and insurers refine their policy language, these coverage issues will become more commonplace, and courts will become more familiar with them. In the interim, it is important that both insurers and policyholders have experienced insurance counsel representing their interests in this new but growing field of insurance.

Alan Rutkin is a partner and long-time management committee member of Rivkin Radler LLP. He has written many articles concerning insurance issues in the cyber area.

Robert Tugander is a partner in the Insurance Coverage Practice Group at Rivkin Radler, where he counsels insurers in complex coverage disputes. He has handled a wide array of insurance matters relating to environmental, toxic torts, intellectual property, and business tort claims.



Gregory J. Klubok is an associate at Rivkin Radler LLP in the Insurance Coverage Practice Group. Before joining Rivkin Radler, Greg was a Senior Court Attorney at the New York Court of Appeals.

1 *See, e.g., Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am.*, 719 F. App'x 701, 702 (9th Cir. 2018).
2 *Medidata Solutions, Inc. v. Federal Ins. Co.*, 729 F. App'x 117, 118-119 (2d. Cir. 2018); *see also American Tooling Center Inc. v. Travelers Cas. & Sur. Co.*, 895 F.3d 455, 459-461 (6th Cir. 2018)
3 *Anton v. Nat'l Sur. Corp.*, 2016 U.S. Dist. LEXIS 108011, at *19-*20 (S.D. Tex. 2016).
4 *Todd v. Vt. Mut. Ins. Co.*, 137 A.3d 1115, 1122 (N.H. 2016).
5 *Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, L.L.C.*, 644 F. App'x 245, 247 (4th Cir. 2016).
6 *Zurich Am. Ins. v. Sony Corp. of Am.*, 2014 N.Y. Misc. LEXIS 5141 (Sup. Ct., N.Y. Cty. 2014).
7 *Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347* F.3d 89, 95-96 (4th Cir. 2003).
8 *Id.* at 96.
9 *Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs, Inc.*, 2012 U.S. Dist. LEXIS 45184, at *10 (M.D. La. 2012). (quotation marks omitted)*; see also Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 802 (8th Cir. 2010).
10 *Recall Total Information Management v. Federal Insurance Co.*, 115 A.3d 458, 460 (Conn. 2015).
11 *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, 2016 U.S. Dist. LEXIS 70749, at *14-15 (D. Ariz. 2016).